**Security Incident Communications Guidelines and Templates**

Contents

[Introduction: How to Use This Template 2](#_Toc524960053)

[Plan Review Chart 2](#_Toc524960054)

[Holding Statement Example 2](#_Toc524960055)

[Holding Statement Template 4](#_Toc524960056)

[Press Release Example 5](#_Toc524960057)

[Press Release Template 6](#_Toc524960058)

[Dark Site Content Guidelines 7](#_Toc524960059)

[External Message Release Approval Form 9](#_Toc524960060)

# Introduction: How to Use This Template

Use this tool as a reference for the types of documents that might be released during an incident. These documents, if used, need to be approved by your legal department. The templates and examples only serve as guidelines to simplify the message creation process for your organization. Delete or replace any grey introductory or example text before printing or distributing.

# Plan Review Chart

|  |  |  |  |
| --- | --- | --- | --- |
| **Date of Revision** | **Name of Reviser** | **Approved By** | **Notes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Holding Statement Example

Holding statements are designed to provide the media with an initial impression of the situation. Oftentimes many details regarding the incident are not yet available.

**FOR IMMEDIATE RELEASE**

**POTENTIAL DATA BREACH AT TECHNOLOGY EXAMPLE INC.**

TORONTO January 1, 2015: Technology Example Inc. confirms that it has received reports of suspicious web activity. Based on the information that is available at this time, the data breach occurred at 1:30AM EST. The IT team indicates that certain client files have been altered but the extent of breach is currently unknown. Technology Example Inc. is suspending all web transactions to protect all users from further security breaches.

The IT team at Technology Example is working around the clock to segregate and eliminate the threat. Customers are encouraged to contact their financial institutions and notify them of the situation.

Technology Example Inc. will be providing further information as soon as it becomes available. Technology Example Inc. will be holding a press conference at CONFERENCE CENTER at 1:00PM EST at TOWN HALL.

For additional information:

**Name:** Jane Doe

**Title:** Chief of Communications

**Organization:** Technology Example Inc.

**Mobile Number:** (999) 999-1111

**Phone Number:** (999) 111-9999

**Email:** [janedoe@techexample.com](mailto:janedoe@techexample.com)

**Website:** [www.techexample.com/darksite](http://www.techexample.com/darksite)

**Channels of additional information:** www.facebook.com/techexample

# Holding Statement Template

**FOR IMMEDIATE RELEASE**

**[Headline]**

Date: [Date of issue]

Time: [Time of issue]

[LOCATION Month Date, Year]: [Company name] confirms that it has received reports of [description of event]. Based on the information that is available at this time, the [event] occurred at [time and location]. [First responders] indicate that [details of the initial response]. [Company name] is currently [emergency response measures] to protect [affected stakeholders].

**[Adapting]:** [if available]

Supporting Info:

**[Instructing]:** [if available]

Supporting Info:

**[Adjusting]:** [if available]

Supporting Info:

[Organization name] will be providing further information as soon as it becomes available. [Provide details of press conferences or media briefings].

For additional information:

**Name:** [Name of designated spokesperson]

**Title:** [Title of designated spokesperson]

**Organization:** [Name of organization]

**Mobile Number:** [Mobile phone of spokesperson]

**Phone Number:** [Phone number of customer service line]

**Email:** [Direct email of response team]

**Website:** [Dark site]

**Channels of additional information:** [Facebook] [Twitter] [Blog]

# Press Release Example

**FOR IMMEDIATE RELEASE**

Contact Name: Jane Doe

Company Name: Technology Example Inc.

Contact Phone Number: (999) 999-1111

Contact Email Address: [janedoe@techexample.com](mailto:janedoe@techexample.com)

**TECHNOLOGY EXAMPLE INC. DISCOVERS DATA BREACH**

TORONTO, January 1, 2018 – Today at 3:30AM EST, Technology Example Inc. confirms that a group of internet activists named “Hackers” successfully compromised the credit and debit records of all Canadian clients.

The IT team at Technology Example is working around the clock to segregate and eliminate the threat. The current estimated time of recovery is six hours, and updates will be provided on all company communication platforms (presented below).

By end of day, a server update will be provided to prevent future security risks. Customers need to log onto their accounts and install the update.

Technology Example will provide credit monitoring for customers who were affected by the breach; more information regarding this service will be available next week.

Based on our current assessment, we strongly encourage customers to update their firewall with Firmware 1234. As well, customers should contact their financial institutions and notify them of the situation.

Technology Example Inc. is working alongside Data Breach Authorities LLC to investigate the cause of the data breach and the areas of vulnerability in the system.

Due to this unfortunate event, Technology Example Inc. will be offering customers a free annual subscription in the following weeks as an apology for the inconvenience this incident has caused.

Our organization recognizes the magnitude of the situation and offers our sincerest apologies. We welcome all customers who want to learn more about the situation to contact our support center.

Phone Number: (999) 111-9999

Website: [www.techexample.com/darksite](http://www.techexample.com/darksite)

Channels of additional information: www.facebook.com/techexample

# Press Release Template

**FOR IMMEDIATE RELEASE**

Contact Name: [Name of designated spokesperson]

Contact Phone Number: [Mobile phone of spokesperson]

Contact Email Address: [Direct email of response team]

**[Headline]**

[LOCATION Month, Date, Year] – [Outlines the release with the 5 Ws (who, what, when, where, why]

**[Adapting]:**

Supporting Info 1:

Supporting Info 2:

Supporting Info 3:

**[Instructing]:**

Supporting Info 1:

Supporting Info 2:

Supporting Info 3:

**[Adjusting]:**

Supporting Info 1:

Supporting Info 2:

Supporting Info 3:

Phone Number: [Customer service line]

Website: [Dark site]

Channels of additional information: [Facebook] [Twitter] [Blog]

# Dark Site Content Guidelines

Use these guidelines as a starting point for what information to include on your dark site. The points below will need to be included on virtually every dark site, but be sure your dark site develops in a logical manner as you scroll down.

[Date of most recent update]

[Opening statement]

Use this section to give a short overview of what happened and your organization’s reaction to the incident. This section is similar to the holding statement, but should use a more personal tone to convey empathy and sincerity.

E.g.

On January 1, 2018, Technology Example Inc. learned of a security incident that exposed personal data of some of our clients. We are presently in the process of notifying those affected by the incident and want to assure those affected by it that Technology Example takes the incident very seriously and will be offering support to those who need it. Technology Example seeks to provide top quality security to its clients and is taking steps to ensure data security measures are improved so that the incident is not repeated in the future.

We wish to thank all of our loyal clients for their understanding during this time. We look forward to resolving this issue and continuing to serve you in the future.

After the opening statement, each section should provide more context or essential information to the section above it. If your explanation of what happened uses technical terms, be sure to add a section that briefly summarizes what those terms mean. Remember, visitors to the site will want to be able quickly find the information they need. Therefore, keep each section as brief as possible to avoid a wall of text that is difficult to read – stick to just the essential information.

**What happened?**On January 1st, 2018, Technology Example discovered evidence of a data breach resulting in the exposure of some clients’ personal data, including payment card information. The breach was the result of an attack by cybercriminals who were able to find a vulnerability in Technology Example’s security protocols. The vulnerability has since been fixed and security measures have been heightened.

**What data was affected?**The attack resulted in the exposure of client’s email addresses, phone numbers, and payment card information. Presently, it appears that the email addresses were exposed for all affected clients. However, payment card information was not exposed in all cases. An investigation is underway to determine the full extent of the payment card exposure.

**Who was affected?**At this time, the breach appears to have affected approximately 1,200 accounts belonging to clients who started using Technology Example’s services between March and July of 2012.

**How do I know if my data was affected?**If your account was created between March and July 2012, you will receive an email notification from Technology Example with the subject line: **Data Breach Results.** Please be advised that these emails will contain text only and will not ask you to enter login information or other personal details. If you are unsure of the legitimacy of the email you have received, please contact the Incident Response Hotline at 555-555-5500.

**How will updates be communicated?**Technology Example will make every effort to send email correspondence to affected clients. However, we encourage **all** clients to monitor this website, which will be updated with new information as it becomes available.

**What is being done?**In addition to increasing overall security at Technology Example, law enforcement has been contacted and informed of the situation. Technology Example empathizes with all of the affected clients and is working with a third party specializing in data breach investigations to determine the full extent of the incident and exactly which accounts were affected.

**What do I need to do now?**At this time, Technology Example is advising all clients to change their account password. However, this is strictly a precautionary measure, as we have no reason to suspect that passwords were compromised during the breach. We simply want the greatest security possible for all our users.

**What services are being offered to those affected?**Technology Example understands that this is a difficult time for our clients and will provide free credit monitoring for affected clients for a period of 3 years.

**Who do I contact for assistance or more information?**All clients seeking more information or assistance are encouraged to call our Incident Response Hotline at 555-555-5500. This line will be available 24 hours a day.  
  
If you have been notified that you were affected by the breach and require assistance please call our Data Protection Officer directly at 555-555-5501 between the hours of 9 am and 9pm Eastern time.

After answering the above questions, it may be appropriate to provide additional details about what is presently known about the incident. Consider also addressing the following:

**Who is responsible for this incident?**This attack is believed to have been carried out by a group of cybercriminals known as “Hackers.” At this time, we do not have any specific details about the group or why Technology Example was targeted.

**Was this a state-sponsored attack?**Presently, there is no evidence to suggest this attack was ordered by a foreign nation.

**What are the risks of this data being exposed?**Because personal information and payment card data were exposed, the main concern is that a criminal may seek to use this information for their own gain, such as making fraudulent credit card purchases or identity theft. If either of these are suspected, report the incident to the proper authorities.

**I’m concerned about the security of my payment card. Is there anything else I can do?**It is a good idea for all affected clients to notify their finical institution that their data was exposed. However, it is not necessary to cancel payment cards at this time. Moreover, free credit monitoring will be provided to those users whose payment card information was exposed.

**How will incidents like this be prevented in the future?**Technology Example takes cybersecurity very seriously, especially when it comes to protecting our clients’ data. We have requested a security audit from a third-party specialist, which is already underway. Rest assured that Technology Example is making it a priority to upgrade their security protocols.

* These guidelines were inspired by the sites used by [Chili’s](http://brinker.mediaroom.com/ChilisDataIncident) and [UnderArmour](https://content.myfitnesspal.com/security-information/FAQ.html)

# External Message Release Approval Form

To ensure the accuracy and consistency of the released messages, it is a best practice to have the legal or the communications department approve the message.

**Document the communications release:**

**□** Message Map/Statement **□** Letter

**□** Press Release **□** Website Content

**□** Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Approval timeline:**

**□** 0-30 Minutes **□** 30 Minutes-2 Hours

**□** 2-5 Hours **□** 1 Day

**□** 2-3 Days **□** \_\_\_\_\_\_\_\_\_\_\_\_

**Changes made/Changes needed:**

**Approval:**

**□** Approved

**□** Approved with minor changes

**□** Not approved, make changes and resubmit

**Approved By:**

**Signature:**

**Date:**

**Time:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.